IV&V of a Space Robotic Mission's Fault Protection System (Presented and published at AIAA)

Mike Choppa, MSIS

Shirley Savarino, TASC

Frank Huy, NASA

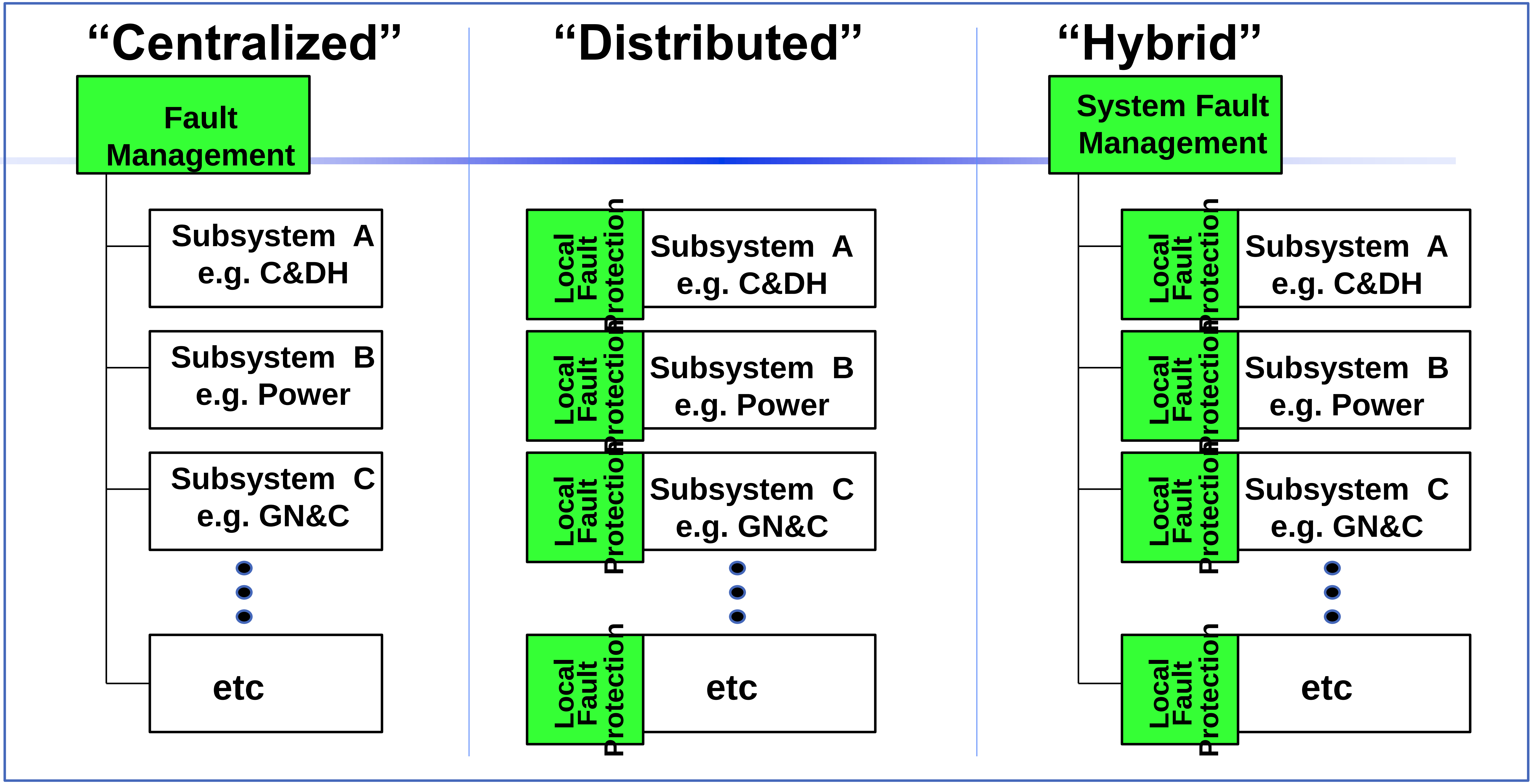
IV&V Annual Workshop

Introduction

- Review IV&V challenges and architectures
- Describe an actual FP architecture and IV&V challenges
- IV&V approaches
  - Monitor Mining
  - Database
- Results and Benefits

Fault Protection – IV&V Challenges

- Last defense prior to loss of mission
- Often, complexity of fault management system correlates to autonomy required by mission type
  - Deep Space and Interplanetary typically require more autonomy than earth observing mission
  - Time-to-criticality also plays a role – GN&C maneuvers have more criticality than operation during a standard orbit
- Fault Protection subsystem is routinely ranked as critical for IV&V analyses
- Scope for IV&V
  - Fault Analysis (safety)
  - Fault Detection, Identification and Response (dependability)



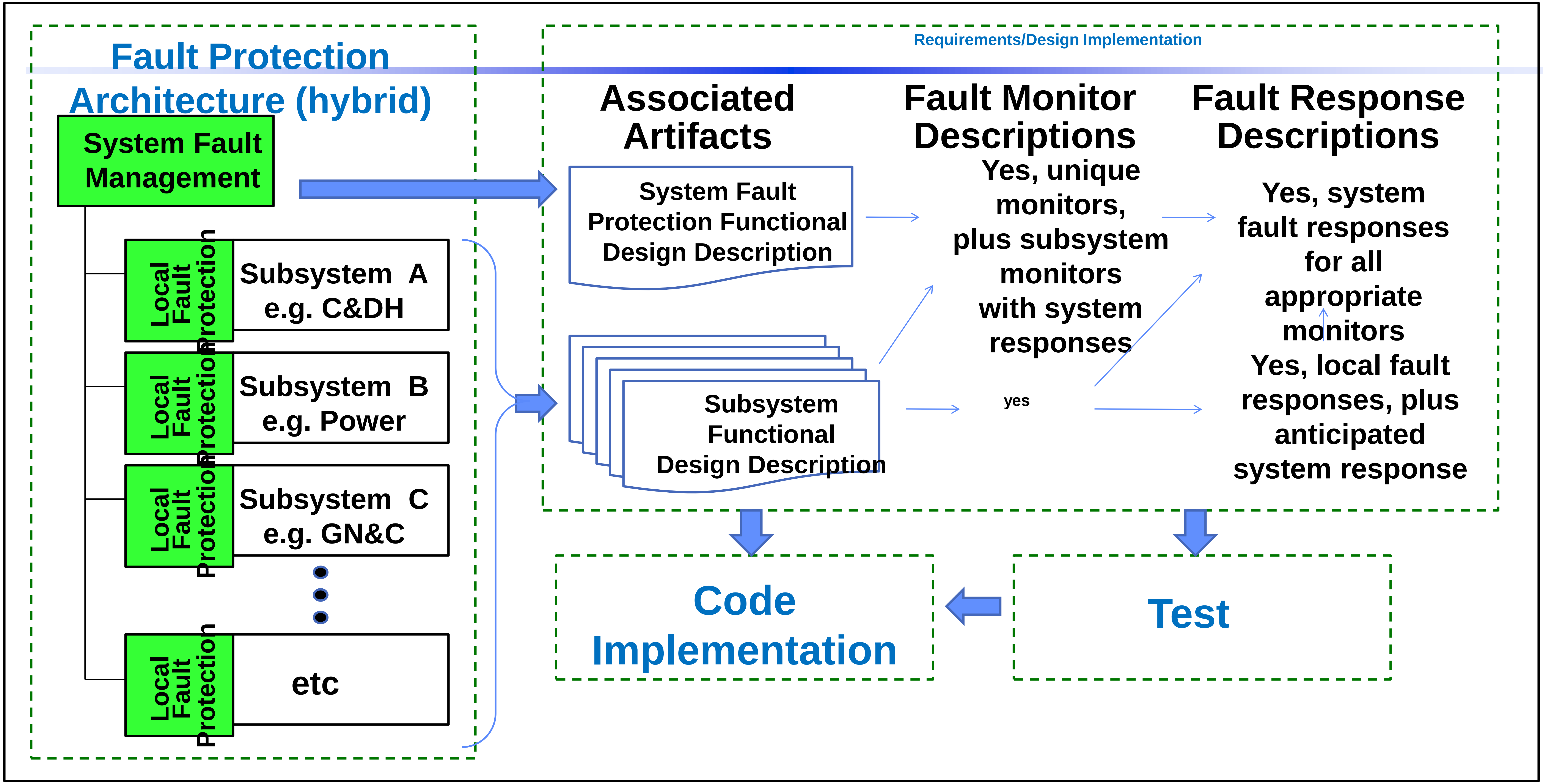
Fault Protection Architecture Types

Fault Protection Architecture Approaches – Advantages and Disadvantages

Type	Description	Advantages	Disadvantages
Centralized	Fault detection monitors and fault responses are located in the primary processor or a single software code unit	Allow for the use of table driven monitors and/or responses. Fault protection verification activities are concentrated to a single implementing subsystem.	Fault detection and responses may be implemented in units removed from the source of the fault, potentially introducing additional failure paths.
Distributed	Fault detection monitors and responses distributed amongst software code units or hardware units.	Allow the fault monitors or fault detection algorithms to be located more closely to the source of the potential failure	Fault protection implementation activities are distributed amongst the subsystems, increasing complexity.
Hybrid	Distributed architecture for fault detection monitors and local responses, combined with a centralized fault response	Both the centralized and distributed advantages apply to this architecture	Complexity is increased over either approach. Fault protection implementation activities are distributed across localized and centralized entities.

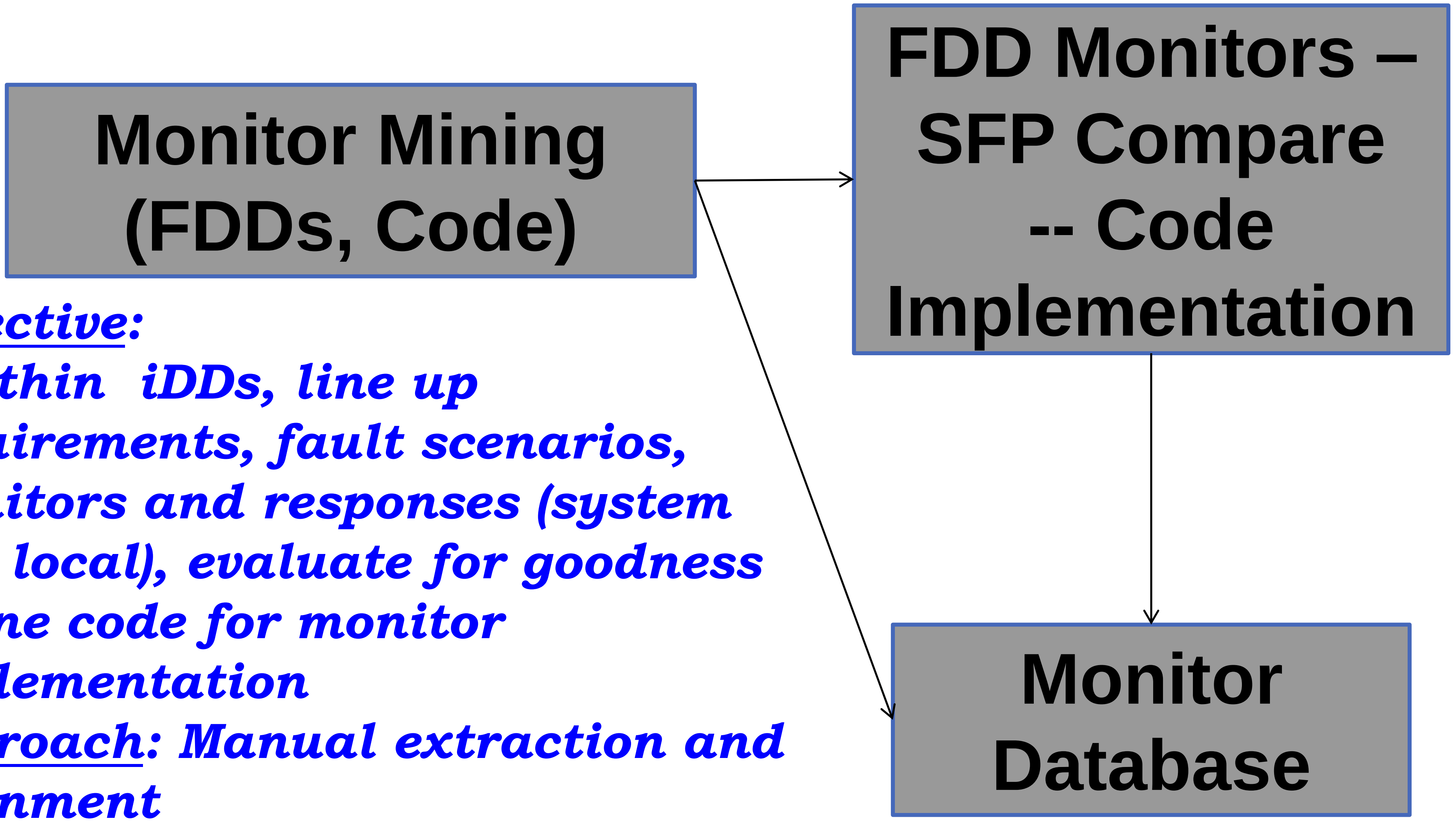
Mars Science Laboratory – Fault Protection Overview

- Leaving for Mars in November, 2011
- Arrives at Mars in August 2012 for a two year surface mission
- Fault protection
  - Uses a hybrid architecture
  - Over 1500 fault monitors with local and system responses
  - Tiered responses (second monitor and associated response if first tier doesn’t work correctly)
- Implementation
  - Requirements/design implemented across 35 Functional Design Documents
  - Distributed implementation in code


Requirements/Design Implementation
Fault Protection Architecture (hybrid)
System Fault Management
Local Fault Protection
Subsystem A e.g. C&DH
Local Fault Protection
Subsystem B e.g. Power
Local Fault Protection
Subsystem C e.g. GN&C
Local Fault Protection
etc
Associated Artifacts
Fault Monitor Descriptions
Fault Response Descriptions
System Fault Protection Functional Design Description
Yes, unique monitors, plus subsystem monitors with system responses
Yes, system fault responses for all appropriate monitors
Subsystem Functional Design Description
yes
Yes, local fault responses, plus anticipated system response
Code Implementation
Test

Hybrid Fault Protection Architecture Implementation Approach

IV&V Monitor Mining Tasks - Approaches


Monitor Mining (FDDs, Code)
FDD Monitors – SFP Compare -- Code Implementation
Monitor Database

Objective:

- Within iDDs, line up requirements, fault scenarios, monitors and responses (system and local), evaluate for goodness
- Mine code for monitor implementation

Approach: Manual extraction and alignment

Summary: identified inconsistent approaches within FDDs, monitors with no responses, incomplete requirements, etc

Code work in progress.

Objective: Ensure SFP identified monitors are being generated at local level and FDD indicated SFP used monitors are used by SFP

Assess consistency in the code

Approach: Automated matches (mnemonics), followed by manual matches

Summary: Identification of orphans and inconsitencies

Objective: Detangle distributed (across artifacts and time) nature of monitors and responses

Approach: Access Database

Summary: Facilitates ongoing analysis (e.g. code trace, new FDDs, change impact and test analysis)

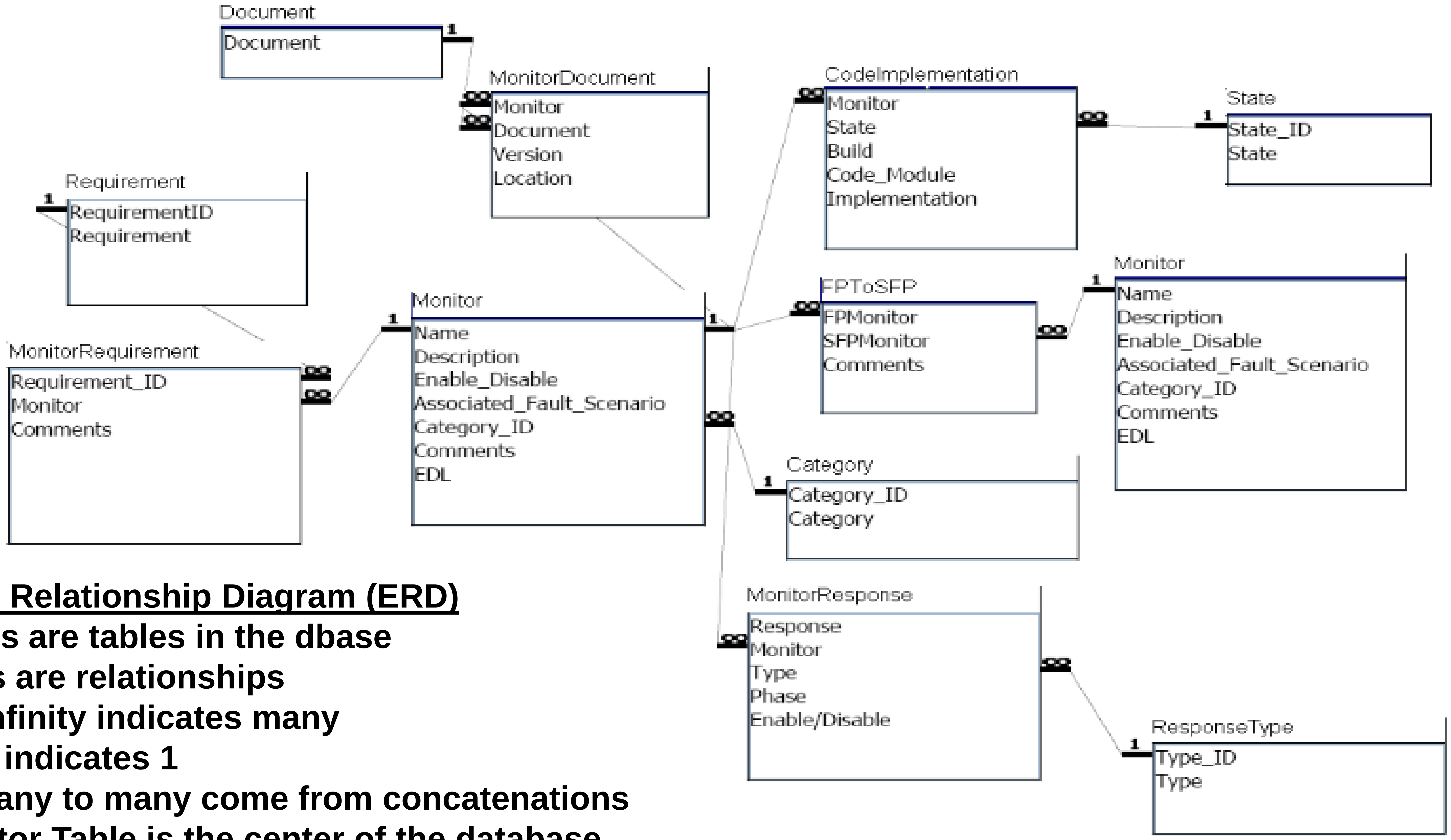
IV&V Monitor Mining Process, Results

Category	Description
IV&V Monitor Mining Work Instructions	• Search the entire FDD for keywords - fault, monitor, response • Review diagrams for fault monitors and responses • Verify implementation of monitors/responses in code (using requirements/design)
IV&V Monitor Mining Result Types	• Missing fault management requirements and/or responses • Incomplete requirements in describing fault scenarios • Requirements with no fault monitor/response • Unclear response descriptions - local or system response • Code implementation is missing local response or has additional steps beyond design description • Code implementation has missing/incomplete event reports • System fault protection handoff in code is incomplete/incorrect

IV&V Monitor Mining Observations

Category	Description
Observations resulting from the IV&V Monitor Mining	• Lexicon: SFP FDD and code uses mnemonics, but subsystem FDDs do not in any consistent fashion. In some cases, monitors are not explicitly named (though fault conditions and responses are provided) – Lack of a consistent lexicon across documentation meant that judgment needed to be applied as to 1) whether a response was truly a fault response or just defensive programming, and 2) uncertainty in the results (though we reviewed and reviewed our work to reduce errors to extent possible) • Different approaches to FP were applied across the FDDs. Faults and associated response descriptions varied across the project. The tables and spreadsheets had the most logical presentations. In some cases faults were only provided in PDF pictures. In other cases, we inferred faults due to telemetry provided

Monitor Mining Database Entity Relationship Diagram



<u>Entity Relationship Diagram (ERD)</u>

-Boxes are tables in the dbase

-Lines are relationships

- **- infinity indicates many**
- **- 1 indicates 1**
- **-Many to many come from concatenations**

-Monitor Table is the center of the database

- **-Dbase differentiates SFP required vs. FDD generated monitors but it is all in the same table**

Monitor Mining Database Benefits

Description	Benefit
Consistency	• Database structure ensures capturing data in a consistent manner
Queries	• Rather than using Excel sorts and filters, database queries can be employed, with results provided in a report
Reports, Input Forms	• Reports capture data in any manner desired • Different reports/input forms can be employed by different analysts as long as the same data is captured
Agility and speed of manipulating data	• Greatly improved over spreadsheet approach - this was perhaps the most important and quickly realized benefit once the monitor mining database was operational • Database allows IV&V to capture analysis and provide reports of remaining efforts. • During analysis, identification of exceptions (issues) are facilitated by database queries • Database enables IV&V to focus on the analysis tasks vs. the data manipulation efforts

Database demo

- Demo
  - 1: Monitor Input form
  - 2: Monitor Report form
  - 3: Monitor queries

- Features
  - Began in Oct 2010, prototyped in Jan 2011, operational in May 2011
  - Central repository for monitor information.
  - Has been used for IV&V purposes and reports are used to communicate to the MSL Project